REMARKS

Claims 1-10 have been canceled herein without prejudice. Claims 11-16 have been amended herein. Claims 11-16 are now pending in the Application. No new matter has been added. Entry of the amendment is respectfully requested. Reconsideration is respectfully requested.

Amendments to Claims

The claims have been amended to retain only claims that relate to the encrypted digital signatures for cookies in a client-server environment. This change defines the claimed subject matter to be primarily directed to the authentication of such cookies in a client-server network. In particular, claims 11-16 have been amended to include reference to a set of servers, each of which is provided with a unique server-identifier. Each server is defined to potentially store a private key in a dynamic memory on that server, only. The server generates cookies for client computers. Each cookie includes the value of server-identifier for the generating server. When any one of the set of servers receives one of the cookies from one of the uniquely identified set of servers, that server is able to use the cookie's server-identifier to access a database to obtain a public key to allow decryption of the digital signature for authentication of the cookie. Claim 11 as amended recites features previously recited in claim 12 relating to the access of a central database for public keys using server-identifiers. Similarly, claim 14 is amended to recite corresponding subject matter. Support for the amendments is found in the specification and original claims.

The Pending Claims Are Not Anticipated or Obvious in View of the Applied Art

Claims 1-16 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Mitsitaka, Japanese Patent #11-98134-A (referred to as '134) in view of Bruce Schneier, "Applied Cryptography" (referred to as "Schneier"). These rejections are respectfully traversed.

The Applied References Do Not Disclose or Suggest the Features and Relationships Recited in Applicants' Claims

Before a claim may be rejected on the basis of obviousness pursuant to 35 U.S.C. § 103, the Patent Office bears the burden of establishing that all the recited features of the claim are known in the prior art. This is known as *prima facie* obviousness. To establish *prima facie* obviousness, it must be shown that all the elements and relationships recited in the claim are known in the prior art. If the Office does not produce a *prima facie* case, then the Applicants are under no obligation to submit evidence of nonobviousness. MPEP § 2142.

The teaching, suggestion, or motivation to combine the features in prior art references must be clearly and particularly identified in such prior art to support a rejection on the basis of obviousness. It is not sufficient to offer a broad range of sources and make conclusory statements. *In re Dembiczak*, 50 USPQ2d 1614, 1617 (Fed. Cir. 1999).

Even if all of the features recited in the claim are known in the prior art, it is still not proper to reject a claim on the basis of obviousness unless there is a specific teaching, suggestion, or motivation in the prior art to produce the claimed combination. *Panduit Corp. v. Denison Mfg. Co.*, 810 F.2d 1561, 1568, 1 USPQ2d 1593 (Fed. Cir. 1987). *In re Newell*, 891 F.2d 899, 901, 902, 13 USPQ2d 1248, 1250 (Fed. Cir. 1989).

The evidence of record must teach or suggest the recited features. An assertion of basic knowledge and common sense not based on any evidence in the record lacks substantial evidence support. *In re Zurko*, 258 F.3d 1379, 59 USPQ2d 1693 (Fed. Cir. 2001).

It is respectfully submitted that the Action does not meet these burdens.

The Pending Claims Are Not Obvious Over
'134 in view of Schneier

In the Action claims 1-16 were rejected under 35 U.S.C. § 103(a) as being unpatentable over '134 in view of Schneier. These rejections are respectfully traversed. Applicants' response to these rejections is based on the Office's referenced interpretation of these references. Thus, any change in the Office's interpretation of '134 and Schneier shall constitute a new ground of rejection.

In the Action, the Examiner refers to the '134 reference as disclosing a "digital signature combined with encryption of cookie" (Section 6, Line 4 *et seq.*, '134). However, the Examiner also concedes that the '134 reference "does not explicitly teach to store the public key in a centralized database available to the set of recipient computers." In fact, there is no discussion in the '134 reference of the issue of multiple servers that each may receive cookies generated by other servers in the client-server network. The '134 reference therefore does not refer to, nor does it suggest solutions to, problems that flow from the use of multiple servers (neither does the '134 reference describe the problem of keeping private keys secret and it does not suggest how to achieve secure storage of these keys).

In contrast, the present application is concerned with a multi-server environment. The application describes the generation of cookies that may be received by server computers other than the computer that generates the cookies. Where the authentication of such cookies is required, there is a need for a mechanism that will permit the digital signature and authentication steps to be carried out. The current application provides a mechanism that is implemented on the server-side of the client-server system only. For the client computers there is no change as to how cookies are handled.

The method and system as claimed provides each of the servers with a unique server-identifier that is included with each encrypted cookie. This server-identifier is also stored in a database in association with the public key that is part of the public-private key pair used in the encryption of the digital signature for the cookie. This server-identifier information is available for use by servers that receive cookies and is used as part of the authentication procedure. The database for public keys is accessible using server-identifiers. Thus servers are able to carry out authentication of cookies that were generated by other servers in the system.

The Examiner suggests that a person skilled in the art would have been motivated to combine the '134 reference and the Schneier reference. However, the '134 reference does not address the issue of multiple servers and the Schneier reference is not concerned with a client-server environment. There would be no motivation to combine these two references. Further, the approach of the present application, giving each server a unique identifier and then including the server-identifier in the cookies generated by the server, is not suggested by either of the cited references, alone or in combination. The inclusion of a server-identifier in cookies and its use in

the management of public keys provides significant advantages in a client-server environment where cookies may be received by different server computers.

It should be noted also that the '134 reference does not suggest the use of a public/private key pair arrangement. Instead, the reference refers to FEAL (Fast data Encipherment ALgorithm) [section 10, lines 5 *et seq.*], which is a symmetric key algorithm for encryption, not an asymmetric public/private key algorithm as is required in the claims of the current application. Thus, the '134 reference that teaches the use of a symmetric encryption, would not lead a person skilled in the art to include the public/private key approach referred to in the Schneier reference.

As indicated in the description, the system of the current application is able to support dynamic public/private key pairs for the same server. By updating the database, a list of current and past public keys for the cookie-generating server is available. This allows cookies to be authenticated (using a past public key) even when the private key in the generating server has been changed. Such authentication can be carried out by the cookie-receiving server computer, whether that computer is the server that generated the cookie originally, or not. Thus in a dynamic client-server environment, the use of the server-identifier and the common database allows historical information to be retained so that previously issued cookies may be authenticated, even when the generating server computer has replaced the original private-public key pair with a new one.

The general approach to key management in Schneier does not teach this dynamic association of public keys with servers in a client-server system or network in which cookies are authenticated. The claims recite the generation of cookies containing the server-identifier for the

server that generated the cookie. There is no suggestion in the cited references to include such information in cookies. The references are not concerned with the problem of authentication in a multi-server environment and therefore do not teach this solution.

It is important to note that the database of public keys is accessible with reference to the server-identifier. The Examiner suggests that the database is to "store keys associated with various users and their corresponding cookies." However, the database does not store keys by their association with users and/or their cookies, but rather the claims recite that the database stores keys in association with the server-identifiers in the system. Such an organizational approach permits the dynamic listing of public keys for a given server and thus seamlessly handles the updating of public/private key pairs for the set of servers in the system. Because of this seamless updating, it is possible to store private keys only in the secure dynamic memories of the servers. This is an important advantage because in a case where the dynamic management of the public-private key pairs is not supported it is necessary to retain the private key in a non-volatile memory with the consequent loss of security. Thus, the approach of the current application permits the secure storage of private keys in dynamic memory, an advantage that flows from the method of dynamic management of the public keys described. Such an advantage is not described nor identified in either of the '134 reference or the Schneier reference.

For the above reasons, it is respectfully submitted that the '134 reference and the Schneier reference do not make obvious the invention as claimed. Favorable reconsideration and allowance of this application are respectfully requested.

Additional Claim Fees

There was no shortened statutory period for reply. Thus no fee is due with the submission of this Response. However, for any other fees due associated with the prosecution of this Application, please charge Deposit Account No. 10-0637 of Walker & Jocke.

Conclusion

Each of Applicants' pending claims specifically recites features and relationships that are neither disclosed nor suggested in any of the applied art. Furthermore, the applied art is devoid of any such teaching, suggestion, or motivation for combining features of the applied art so as to produce Applicants' invention. Allowance of all of Applicants' pending claims is therefore respectfully requested.

The undersigned will be happy to discuss any aspect of the Application by telephone at the Examiner's convenience.

Respectfully submitted,

Ralph E. Jocke Reg. No. 31,029
231 South Broadway
Medina, Ohio 44256
(330) 721-0000